

**REMARKS**

The Applicants request reconsideration of the rejection.

Claims 1-28 are now pending.

Claims 1-2, 4, 19 and 22 were rejected under 35 U.S.C. 102(e) as being anticipated by Trossen et al., U.S. 2004/0153552 (Trossen). The Applicants traverse as follows.

Trossen is directed to access right control using alerts in, for example, an instant messaging environment. Trossen describes two embodiments in which access to “events” is controlled according to a subscription current access control information. In one embodiment, access to information indicating whether a “buddy” is available for communication is provided to users of a certain access level. In a second embodiment, location information of a mobile user is provided, based on access control.

Notably, however, Trossen fails to teach or fairly suggest access control to an information resource stored in a storage device, wherein a plurality of the access controllers and storage devices are connected via a network, such that the access controller restricts access to each information resource stored in a storage device according to an access control list maintained by the access controller. The office action cites Trossen’s “white list” that identifies users that are allowed to subscribe. However, in the example given in Paragraph [0047], SIP event server 14 maintains location information of the user’s mobile device, and implements a cache of access rights for a location “event” as well as other applicable events. According to this

embodiment, a requestor may attempt to subscribe to the “event” of the location of the mobile device, but the “event” does not correspond to the claimed information resource stored in a storage device. More specifically, Trossen’s control of access to the location of a mobile user does not constitute control of access to an information resource stored in a storage device, restricted according to an access control list on which access right to each information resource and plural storage devices in the network is recorded.

The Applicants further note, in the Office Action, the rejection based on Trossen’s alleged teaching of an access interception module configured to intercept an access by an access prohibited user listed on an access prohibition list (the Office Action citing Trossen’s “black list”), and an input module configured to input user information corresponding to the access prohibited user (citing Trossen’s changing of access rights “which would require inputting user information corresponding to the user on a black list”). However, Trossen does not teach that a black list, any module implementing the black list, or any module configured to input user information, forms part of an access controller with any access restriction module alleged to implement the white list.

Furthermore, whereas the invention requires a list update module configured to update the access prohibition list, or a step for updating the access prohibition list, corresponding to each access controller connected with the network, Trossen is alleged to show subscription commands that allow for the changing of access rights, distributed access controllers and updating thereof, and submitting and updating of

access rights. Trossen's Paragraph [0032], however, discloses a single alert event server 12 that stores the subscription for a specified event in a local database 35 stored in memory 34. Trossen's Paragraph [0039] discloses plural local repositories 27 that receive "appropriate" match messages 116 based on various factors, which does not comport with the claimed requirement that the access prohibition list of each access controller be updated according to the user information input through the input module. Further, Paragraph [0051] generally describes message flow where access is allowed, access is unclear, or there are no access rights. Thus, Trossen does not disclose or suggest the claimed update module or method step of updating the access prohibition list corresponding to each access controller according to the user information.

Concerning Claim 2, the Office Action asserts that Trossen teaches, in Paragraphs [0039] and [0032], an access controller having a list update module that sends out to other access controllers a registration instruction to register the input user information on the access prohibition list on the other access controllers. The rejection asserts that these paragraphs identify a SUBSCRIBE message "as being capable to update or change the access rights," and "sending the update messages to multiple access controllers and when the updated list is the black list, updating the black list." Concerning the first quoted passage, mere capability to update or change access rights does not meet the claim limitation of sending to other access controllers a registration instruction to register input user information on the access prohibition list of the other access controllers. Concerning the second quoted

passage, Paragraph [0039] does not disclose sending update messages to multiple access controllers and updating the black list accordingly. Rather, this paragraph discloses that a repository may be identified in the SUBSCRIBE message 40, or that a repository may be identified by another method of identifying an appropriate repository for receiving a match message 116. The paragraph also discloses that alert event server 12 may query the access rights with all associated local repositories by sending appropriate match messages 116 to all associated repositories or agents and if the repository functionality is co-located with alert event server 12, match message 116 might not need to be sent. The paragraph does not disclose sending update messages to multiple access controllers or updating the black list.

Claim 3 was rejected under 35 U.S.C. 103 as being unpatentable over Trossen in view of Herland, U.S. 2003/0018747 (Herland). As noted by the Examiner, and as asserted by the Applicants against the rejection of claims 1-2, 4, 19 and 22 above, Trossen does not disclose a list update module that sends out updated access prohibition list information to other access controllers. In the rejection of Claim 3, the Office Action asserts that Herland discloses such a list update module, citing Paragraph [0034] and the expression send an updated list of users. According to the rejection, this passage shows that sending a list of data between two objects is well known in the art, and thus it would have been obvious to modify Trossen according to Herland for the purpose of sending a list of data between two points. Continuing this chain of reasoning, the rejection then asserts

that the ordinarily-skilled artisan would have been motivated to improve the invention of Trossen such that an updated list of prohibited users could be sent to another access controller.

Respectfully, this chain of reasoning fails on several grounds. First, Herland is directed to a web presence detector that detects one or more user presences on, for example, a website accessed by plural users. Essentially, each user of the website is tracked by a tracking server, and the presence of each user on the website is displayed to each other user of the website. In this regard, Paragraph [0034] does indeed show that an updated list of users is sent to each user on the web page at a given time.

However, it is improper to broaden this specific teaching to find obvious any sending of any list of data between any two objects so as to find Claim 3 obvious. Moreover, there is simply no support in Herland for Trossen to then narrow the breadth of this finding to decide it obvious to the person of ordinary skill to improve Trossen's event access control scheme to pass an updated list of prohibited users between access controllers. Neither Trossen nor Herland discloses that an updated list of prohibited users should be passed between access controllers. Trossen suggests, at most, the updating of a list of prohibited users, and Herland suggests, at most, the display of a current list of users. Indeed, Herland's list is a list of approved users. Neither reference suggests that a list of prohibited users should be passed among access controllers, and thus no motivated combinations of teachings of these two references suggests such a swap of prohibited users.

Claims 5-8 were rejected under 35 U.S.C. 103(a) as being unpatentable over Trossen in view of Wilson et al., 2003/0041088 (Wilson).

Wilson is cited as disclosing an access control list update module configured to update an access control list according to an access prohibition list. In the invention, the access control list records the access right to each information resource stored in a storage device, according to which the access restriction module restricts access to the information resources. The access prohibition list is different in that the access prohibition list contains identifiers of users whose access is intercepted or prohibited entirely.

Wilson is cited for a single Paragraph [0245], allegedly teaching to update a first list based on the changes occurring in a second list. Respectfully, Claims 5-8 are not recited so broadly as to encompass all updating of a first list based on the changes occurring in a second list. Indeed, Wilson's update of an allocated resource list based on a temporary list developed during an arbitration process is wholly irrelevant to both the claimed invention and to Trossen. Thus, the Applicants submit that it would not have been obvious to the person of ordinary skill to modify Trossen according to Wilson to maintain data consistency between two changing lists of users, because Trossen does suggest the need for such an improvement, and Wilson's list updating is not consistent with the white list of Trossen. Indeed, Trossen does not teach that the white list is updated in accordance with the black list at all.

Concerning Claim 6, the claim requires the list update module to delete the user information on the access prohibition list at a predetermined timing. Against this limitation, the Office Action asserts Trossen's teaching that when a subscription expires, access rights are dissolved. However, it is the user information on the access prohibition list that is being deleted (that is, prohibition information) not access rights. Thus, Trossen's Paragraph [0032] does not teach "exactly what the Applicant is claiming here."

Concerning Claims 7 and 8, the Applicants respectfully submit that there is no functionality in Trossen that is identical to the functionality of any claimed element presented by the Applicants. Claims 7 and 8 are patentable for reasons similar to those advanced above.

Claims 9, 15, 18, 20-21 and 23 were rejected under 35 U.S.C. 103(a) as being unpatentable over Trossen in view of Wang, U.S. 2004/003589 (Wang). Essentially, each of these independent claims is rejected on a similar basis advanced above with respect to Claim 1, with Wang alleged to teach restriction of access by reference to an access prohibition list prior to an access control list. The Applicants traverse as follows.

As noted above, the claimed access control list records access rights to each information resource such that access to the information resources is restricted according to the list. On the other hand, the access prohibition list contains information of users whose access is intercepted or prohibited.

Wang's Paragraph [0033] discloses that, if no match is found in an operator black-list, a receiver white-list is searched for an entry matching the sender to 10 with the originating message 215. If a match is found, than a "TRUSTED" annotation is added to the message 215. If no match is found, the operator white-list is searched for a match. If a match is found in the operator white-list, than a "TRUSTED" annotation is added to the message 215. If no match is found, than an "UNTRUSTED" annotation is added to the message 215.

Wang, however, is not applicable as a secondary reference in combination with Trossen. Note that Trossen is directed to control of access to an event such as the presence of a "buddy" or the location of a mobile user. Wang is entirely directed to a method and system for controlling messages passed in a communication network, such that unwanted or untrusted (for example, junk or spam) messages are either rejected or identified as such. Thus, Wang neither discloses nor suggests control of access to an information resource in a storage device. At most, an attempt to combine the teachings of Wang with Trossen would result in Trossen being modified to permit rejection or identification of unwanted messages passing in the instant messaging network of Trossen. Trossen would then retain the deficiencies noted above that are required to render obvious the claimed invention.

Each of the other independent claims rejected over Trossen in view of Wang contains structure or function also requiring the reference to the access prohibition list prior to reference to the access control list. As noted in the present specification, reference to the access prohibition list potentially saves processing in that a



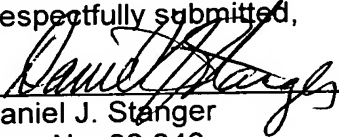
prohibited user is identified immediately without recourse to the much larger access control list, which contains the access right information for each information resource. Wang's disclosure does not necessarily provide this advantage, but instead is directed to a two-stage (and thus) slower attempt to ensure that an attempt to transmit an unwanted message is not successful.

Claims 11-14 were rejected under 35 U.S.C. 103(a) as being unpatentable over Trossen in view of Wang and Wilson. Each of these references having been distinguished above, the Applicants submit that their combination also fails to render obvious the invention claimed in Claims 11-14 for similar reasons.

News Claims 24, 27, and 28 are independent claims that recite many of the above-mentioned features in terms of varying scope. Together with dependent Claims 25 and 26, new Claims 24-28 are thus patentable over the prior art for those reasons similar to those advanced above.

In view of the foregoing amendments, remarks, and new claims, the Applicants request reconsideration of the rejection and allowance of the claims.

Respectfully submitted,

  
\_\_\_\_\_  
Daniel J. Stanger  
Reg. No. 32,846

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.  
1800 Diagonal Rd., Suite 370  
Alexandria, Virginia 22314  
(703) 684-1120  
Date: February 15, 2006